대한민국특허청
KOREAN INTELLECTUAL PROPERTY OFFICE

별첨 사본은 아래 출원의 원본과 동일함을 증명함.

This is to certify that the following application annexed hereto is a true copy from the records of the Korean Intellectual Property Office.

출 원 번 호 : 특허출원 2003년 제 0101775 호
Application Number 10-2003-0101775

출 원 년 월 일 : 2003년 12월 31일
Date of Application DEC 31, 2003

출 원 인 : 주식회사 잉카인터넷
Applicant(s) INCA INTERNET CO., LTD.

2005 년 1 월 10 일

특 허 청
COMMISSIONER

【서지사항】

【서류명】	특허출원서
【접리구분】	특허
【수신처】	특허청장
【출원일자】	2003.12.31
【발명의 명칭】	신뢰할 수 있는 프로세스를 허용하는 유연화된 네트워크 보안 시스템 및 그 방법
【발명의 영문명칭】	Flexible network security system and method to permit trustful process
【출원인】	
【명칭】	주식회사 잉카인터넷
【출원인코드】	1-2000-026490-8
【대리인】	
【성명】	전영일
【대리인코드】	9-1998-000540-4
【포괄위임등록번호】	2002-040650-4
【발명자】	
【성명의 국문표기】	이동혁
【성명의 영문표기】	LEE,Dong Hyuk
【주민등록번호】	750512-1953122
【우편번호】	156-846
【주소】	서울특별시 동작구 상도동 299-41번지, 302호
【국적】	KR
【심사청구】	청구
【취지】	특허법 제42조의 규정에 의한 출원, 특허법 제60조의 규정에 의한 출원심사 를 청구합니다. 대리인 전영일 (인)
【수수료】	
【기본출원료】	20 면 29,000 원
【가산출원료】	10 면 10,000 원
【우선권주장료】	0 건 0 원
【심사청구료】	10 항 429,000 원

【합계】 468,000 원

【감면사유】 중소기업

【감면후 수수료】 234,000 원

【첨부서류】 1. 요약서·명세서(도면)_1통 2.중소기업기본법시행령 제2조에의한 중소기업에 해당함을 증명하는 서류_1통

【요약서】

【요약】

본 발명은 신뢰할 수 있는 프로세스를 허용하는 유연화된 네트워크 보안 시스템 그 방법에 관한 것이다.

본 발명에 따르면, 네트워크 상에서 통신하기 위한 프로그램이 사용하는 서버 트 정보, 프로토콜 정보 및 오픈/클로우즈(Open/Close) 정보를 추출하는 포트 감시 단; 네트워크 사이에서 통신되는 정보의 제한 조건을 설정함으로써, 네트워크에 연 된 컴퓨터의 해당 네크워크 연결을 보호하는 방화벽(Firewall) 수단; 상기 방화벽 단에서 통신을 허용하는 프로그램에 대한 정보를 추출하여 이를 등록하는 내부 허 프로그램 저장 수단; 상기 내부 허용 프로그램 저장 수단에 등록되어 있는 프로그 이 사용하는 오픈된 서버 포트에 대한 정보를 추출하여 등록하는 내부 허용 포트 장 수단; 및 인바운드(Inbound)된 트래픽 패킷의 목적지 포트가 상기 내부 허용 포 저장 수단에 등록되어 있는지 여부를 판단하여, 등록되지 아니한 포트이면 상기 화벽 수단으로 전송하고, 등록되어 있는 포트이면 해당 패킷을 직접 해당 프로그램 전송하는 방화벽 유연화 수단; 을 포함하는 것을 특징으로 하는 신뢰할 수 있는 로세스를 허용하는 네트워크 보안 시스템이 제공된다.

【대표도】

도 6

【색인어】

넷 연결 방화벽, 스텔쓰, 후킹, NDIS

【명세서】

【발명의 명칭】

신뢰할 수 있는 프로세스를 허용하는 유연화된 네트워크 보안 시스템 및 그 방법

exible network security system and method to permit trustful process】

【도면의 간단한 설명】

도 1은 마이크로소프트(Microsoft) 사에서 윈도우 엑스피(Windows XP) 버전부터 기본적으로 제공하는 해당 컴퓨터와 네트워크를 보호하기 위한 인터넷 연결 방화벽(ICF : Internet Connection Firewall)을 보여주는 도면이고.

도 2는 윈도우즈 엑스피에서 서버로 등작하는 소프트웨어가 사용하는 포트. 프로토콜. 아이피(IP : Internet Protocol) 등을 추가하는 인터페이스 화면을 보여주는 도면이고.

도 3은 본 발명에 이용되는 마이크로소프트 윈도우즈 운영 체제의 모드 구분 블록도이고.

도 4는 본 발명에 따른 인터넷 연결 방화벽의 동작을 간략화한 흐름도로서. 포트 감시부와 인터넷 연결 방화벽 설치 및 허용 프로그램 목록을 내부 허용 프로그램 저장소에 저장하는 과정을 나타낸 흐름도이고.

도 5는 본 발명의 일 실시예에 따른 유연한 인터넷 연결 방화벽에서 통신 허용 프로그램 목록을 내부 허용 프로그램 저장소에 저장하기 위하여 디스플레이되는 인터페이스 화면을 보여주는 도면이고.

도 6은 본 발명에서 제시하는 인터넷 연결 방화벽 유연화 장치를 사용하는 전체 }화벽의 동작을 보여주는 블록도이고.

도 7은 본 발명의 일 실시예에 따른 유연한 인터넷 연결 방화벽의 내부 허용 포 저장소에 서버 포트를 저장하고 삭제하는 과정을 나타낸 흐름도이다.

발명의 상세한 설명】

발명의 목적】

발명이 속하는 기술분야 및 그 분야의 종래기술】

본 발명은 신뢰할 수 있는 프로세스를 허용하는 유연화된 네트워크 보안 시스템 그 방법에 관한 것으로서. 보다 상세하게는. 인터넷 연결 방화벽에 통신이 허용 프로그램이 사용하는 포트를 자동으로 추가 및 제거를 하게 함으로써. 전문 사용가 아닌 일반 사용자들도 쉽게 우수한 기능의 인터넷 연결 방화벽을 사용할 수 있끔 하는 네트워크 보안 시스템 및 그 방법에 관한 것이다.

방화벽(Firewall)은 네트워크와 외부 세계 사이의 보호 경계선과 같은 보안 시템이다.

도 1은 마이크로소프트(Microsoft) 사에서 윈도우 엑스피(Windows XP) 버전부터 |본적으로 제공하는 해당 컴퓨터와 네트워크를 보호하기 위한 인터넷 연결 방화벽 CF : Internet Connection Firewall)을 보여주는 도면이다.

이러한 인터넷 연결 방화벽은 네트워크 또는 소규모 네트워크와 인터넷 사이에 신되는 정보의 제한 조건을 설정하는데 사용되는 소프트웨어로서, 인터넷에 연결된 일 컴퓨터의 해당 인터넷 연결을 보호한다.

한편, 종래의 인터넷 연결 방화벽은 '상태 저장' 방화벽이다. 상태 저장 방화 이라 함은 해당 경로를 통과하는 통신의 모든 부분을 모니터링하고, 처리되는 각 시지의 원본, 대상 주소 및 포트를 검사하는 방화벽이다.

인터넷 연결 방화벽은 아웃바운드(Outbound) 트래픽은 허용하고, 인바운드 nbound) 트래픽은 차단함으로써, 네트워크 상에서 외부로부터 보이지 않게 하기 때에 개인용 PC 방화벽에서는 이 기능을 스텔쓰(Stealth) 기능이라고도 한다.

인터넷 연결 방화벽의 동작을 간략하게 소개하면, 다음과 같다.

인터넷 연결 방화벽은 원하지 않는 트래픽이 개인 연결로 입력되지 않도록 하기 하여 인터넷 연결 방화벽 컴퓨터에서 시작된 트래픽을 추적하여 모든 통신 테이블 보관한다. 그리고, 인터넷의 모든 인바운드 트래픽은 테이블에 있는 항목과 비교 다. 인바운드 인터넷 트래픽은 테이블에 일치하는 항목이 있어서 통신 교환이 사 자의 컴퓨터에서 시작되었음을 입증하는 경우에만 네트워크 컴퓨터에 연결된다.

인터넷 연결 방화벽은 인터넷 접속이 방화벽 허용 목록에서 허용되지 아니한 것 면, 연결이 끊어지도록 한다. 따라서, 원하지 않는 통신을 자동으로 소함으로써, 포트 스캐닝(Port Scanning)과 같은 일반적인 해킹을 차단할 수 있게 다.

가령, 이러한 예를 알아 보기 위해서, 인터넷 연결 방화벽 컴퓨터를 리눅스 inux)의 nmap 스캐닝 툴로 스캔을 하면, 인터넷 연결 방화벽 컴퓨터가 모든 스캔 작에 응답하지 않기 때문에 nmap은 모든 스캔에 대하여 타겟 컴퓨터가 네트워크 상 존재하지 않는 것으로 판단하여, 'Host Seems Down'이라는 메시지를 출력한다. 와 같이 인터넷 연결 방화벽은 원하지 않는 통신을 자동으로 취소하여 포트 스캐닝 같은 일반적인 해킹을 차단한다.

한편, 웹 서비스를 제공하는 컴퓨터에 인터넷 연결 방화벽이 설치되면, 이러한 터넷 연결 방화벽이 인바운드 트래픽을 차단하기 때문에, 인터넷 연결이 끊겨 정상인 웹 서비스를 제공할 수 없게 된다. 이를 해결하기 위하여 인터넷 연결 방화벽 서비스가 사용하는 80번 포트로 인바운드 트래픽을 허용함으로써, 정상적인 웹 서스를 제공할 수 있다.

이와 같이 인터넷 연결 방화벽은 서비스와 프로토콜을 추가함으로써, 정상적인 비스를 사용할 수 있고, 개인용 PC 방화벽에서도 이와 같은 기능들을 제공한다.

한편, 이러한 인터넷 연결 방화벽에 있어서의 문제점을 살펴 보면, 다음과 같다

웹 서버, FTP(File Transfer Protocol) 서버, 텔넷(Telnet) 서버, P2P(Peer to er) 프로그램, 원격 제어 프로그램, 메신저 프로그램 등의 최근의 인터넷 사용 소트웨어들은 서비스를 제공하는 서버로 동작한다. 그리고, 이와 같이 서버로 동작

는 소프트웨어들의 수는 급격하게 증가하고 있으며, 일반 사용자들도 이러한 소프
웨어를 많이 사용하고 있는 추세이다.

그러나, 대부분의 사용자들은 위와 같이 서버로 동작하는 소프트웨어들이 정상
으로 작동하지 않기 때문에 인터넷 연결 방화벽이나 개인용 PC 방화벽의 스텔쓰 기
사용을 기피하고 있다. 물론, 도 2와 같이 윈도우즈 엑스피에서는 서버로 동작하
소프트웨어가 사용하는 포트, 프로토콜, 아이피(IP : Internet Protocol) 등을 추
함으로써, 해당 소프트웨어를 정상적으로 사용할 수 있다. 그러나, 전문가가 아닌
일반 사용자들이 이를 설정하기에는 어려운 것이 또한 현실이다. 왜냐하면, 전문가
아닌 일반 사용자들이 서버로 동작하는 포트를 알아내기는 힘들기 때문이다.

또한, 이러한 소포트웨어들의 버젼이 업그레이드될 때마다 서버로 사용하던 포
는 변경될 수 있기 때문에 불의에 정상적인 서비스가 중단될 수도 있다.

이와 같이 여러가지 이유로 말미암아 인터넷 연결 방화벽은 개인용 PC 방화벽의
스텔쓰 기능이 우수함에도 불구하고, 일반 사용자들이 사용하기에는 어렵다는 문제
이 있다.

발명이 이루고자 하는 기술적 과제】

상기와 같은 종래 기술의 문제점을 해결하기 위한 본 발명의 목적은 인터넷 연
방화벽에 통신이 허용된 프로그램이 사용하는 포트를 자동으로 추가 및 제거를 하
함으로써, 전문 사용자가 아닌 일반 사용자들도 쉽게 우수한 기능의 인터넷 연결

화벽을 사용할 수 있게끔 하는 네트워크 보안 시스템 및 그 방법을 제공하기 위한
이다.

[발명의 구성 및 작용]

상기한 목적을 달성하기 위하여 본 발명에 따르면, 네트워크 상에서 통신하기
한 프로그램이 사용하는 서버 포트 정보, 프로토콜 정보 및 오픈/클로우즈
pen/Close) 정보를 추출하는 포트 감시 수단; 네트워크 사이에서 통신되는 정보의
한 조건을 설정함으로써, 네트워크에 연결된 컴퓨터의 해당 네크워크 연결을 보호
는 방화벽(Firewall) 수단; 상기 방화벽 수단에서 통신을 허용하는 프로그램에 대
정보를 추출하여 이를 등록하는 내부 허용 프로그램 저장 수단; 상기 내부 허용
로그램 저장 수단에 등록되어 있는 프로그램이 사용하는 오픈된 서버 포트에 대한
보를 추출하여 등록하는 내부 허용 포트 저장 수단; 및 인바운드(Inbound)된 트래
패킷의 목적지 포트가 상기 내부 허용 포트 저장 수단에 등록되어 있는지 여부를
단하여, 등록되지 아니한 포트이면 상기 방화벽 수단으로 전송하고, 등록되어 있는
트이면 해당 패킷을 직접 해당 프로그램에 전송하는 방화벽 유연화 수단; 을 포함
여 이루어진 것을 특징으로 하는 신뢰할 수 있는 프로세스를 허용하는 네트워크 보
시스템을 제공한다.

또한, 네트워크 사이에서 통신되는 정보의 제한 조건을 설정함으로써, 네트워크
연결된 컴퓨터의 해당 네크워크 연결을 보호하는 방화벽(Firewall)을 이용하는 네
워크 보안 방법에 있어서, 네트워크 상에서 통신하기 위한 프로그램이 사용하는 서
포트 정보, 프로토콜 정보 및 오픈/클로우즈(Open/Close) 정보를 추출하는 제 1

계: 통신을 허용하는 프로그램에 대한 정보를 추출하여 등록하는 제 2 단계: 상기 2 단계에서 등록되어 있는 프로그램이 사용하는 오픈된 서버 포트에 대한 정보를 출하여 등록하는 제 3 단계: 인바운드(Inbound)된 트래픽 패킷의 목적지 포트가 상 제 3 단계에서 등록되어 있는지 여부를 판단하는 제 4 단계: 상기 제 4 단계에서 판단 결과, 등록되지 아니한 포트이면, 상기 방화벽으로 전송하는 제 5 단계: 및 기 제 4 단계에서의 판단 결과, 등록되어 있는 포트이면, 해당 패킷을 직접 해당 로그램에 전송하는 제 6 단계: 를 포함하는 것을 특징으로 하는 방화벽을 이용하는 트워크 보안 방법을 제공한다.

보다 더 양호하게는, 상기 제 1 단계는, TCP(Transmission Control Protocol)를 용하는 통신인 경우, 소켓이 서버로 동작하기 위하여 리슨(Listen)을 수행할 때, 킹(Hooking)을 함으로써 리슨 포트를 추출한다.

또한, 보다 더 양호하게는, UDP(User Datagram Protocol)를 이용하는 통신인 경 , 소켓에서 패킷을 받기 위하여 관련 함수를 호출하면, 유저 모드(User Mode)에서 킹을 함으로써, 서버 포트를 추출한다.

이하, 첨부된 도면을 참조하면서 본 발명의 일 실시예에 따른 신뢰할 수 있는 로세스를 허용하는 유연화된 네트워크 보안 시스템 및 그 방법을 보다 상세하게 설 하기로 한다.

먼저, 본 발명의 백그라운드에 해당하는 관련 기술들을 간략히 살펴 보도록 한

도 3은 본 발명에 이용되는 마이크로소프트 윈도우즈 운영 체제의 모드 구분 를 도이다.

도 3을 참조하면, 마이크로소프트사에서 제공하는 윈도우즈 엑스피는 커널 드(Kernel Mode)와 유저 모드(User Mode)로 나누어지는데, 커널 모드에서는 운영 제 커널과 각종 디바이스 드라이버(Device Driver)가 구동되고, 유저 모드에서는 로 어플리케이션(Application)이 구동된다. 그리고, 커널 모드에서 동작을 하는 로그램들은 디바이스 드라이버의 형태로 존재한다.

마이크로소프트 윈도우즈 운영 체제의 커널 모드 네트워크 구조는 윈도우즈 소 (Socket)의 커널 부분인 AFD(afd.sys), NDIS(네트워크 드라이버 인터페이스 명세 : twork Driver Interface Specification) 및 TDI(전송 드라이버 인터페이스 : ansport Driver Interface)로 구성된다.

커널 모드에서 최상위 계층에 존재하는 afd.sys는 윈도우즈 소켓에서 유저 모드 최하위 계층의 DLL(동적 연결 라이브러리 : Dynamic Link Library)인 msafd.dll과 통신을 하고, 아래 계층의 TDI와 인터페이스를 이루게 된다.

TDI는 프로토콜 스택(Stack)의 상위에 존재하는 커널 모드 인터페이스를 정의한 . NDIS는 NIC 디바이스 드라이버(Network Interface Card Device Driver)들을 위 여 표준 인터페이스를 제공한다.

마이크로소프트사의 윈도우즈 운영 체제의 유저 모드에서 방화벽을 만드는 방법 간단하게 설명한다.

후킹(Hooking)이란 후킹하려는 함수의 원본 주소를 저장하고, 자신이 만든 함수 주소로 교체한 후, 자신의 함수를 먼저 실행하도록 함으로써, 나중에 원본 함수를 실행하게 하는 널리 알려진 프로그래밍 방법이다.

(1) LSP(Winsock Layered Service Provider) : 이 방법은 마이크로소프트사에서 공하는 방법으로서, QOS(Quality Of Service), URL 필터링 및 데이터 스트림(Data ream)의 암호화에 많이 사용되는 마이크로소프트 네트워킹에 있는 컴포넌트인 I(Service Provider Interface)를 기반으로 한다.

(2) 윈도우즈 2000 패킷 필터링 인터페이스(Windows 2000 Packet Filtering terface) : 윈도우즈 2000은 유저 모드의 응용 프로그램이 아이피 주소 및 포트 정를 기반으로 허용/차단할 수 있도록 필터 디스크립터(Filter Descrypter)를 설치하 방법을 이용한 것이다.

(3) Winsock Dll 교체 : 마이크로소프트 윈도우즈의 Winsock DLL을 사용자가 만 DLL로 교체하여 필터링을 하는 방법을 기반으로 한다.

(4) 글로벌 함수 후킹(Global Function Hooking) : 커넥트(Connect), 리슨 isten), 센드(Send), 리시브(Recv), 센드투(Sendto), 리시브 프롬(Recvfrom)과 같 윈도우즈의 소켓 함수를 후킹 또는 유저 모드의 어플리케이션이 커널 모드의 드라 버와 통신하기 위하여 사용하는 DeviceIoControl() 함수를 후킹하는 방법을 기반으 한다.

마이크로소프트사의 윈도우즈 운영 체제의 커널 모드에서 방화벽을 만드는 방법 간단하게 설명한다.

(1) 커널 모드 소켓 필터(Kernel Mode Socket Filter) : 유저 모드에서 윈도우 소켓의 최하위 계층의 DLL인 msafd.dll이 커널 모드 윈도우즈 소켓인 afd.sys와 신하는 모든 I/O를 후킹하는 방법을 기반으로 한다.

(2) TDI 필터 드라이버 : tcpip.sys 드라이버(₩Device₩RawIp, ₩Device₩Udp, evice₩Tcp, ₩Device₩Ip, ₩Device₩MULTICAST)에 의하여 생성된 디바이스에 AttackDevice() API를 사용하여 필터 드라이버로 적용하는 방법이다. 또는, pip.sys의 드라이버 오브젝트(Driver Object)에 있는 디스패치 테이블(Dispatch ble)을 바꿔치기하여 모든 I/O를 후킹하는 기법을 기반으로 한다.

(3) NDIS IM(InterMediate) 드라이버 : 마이크로소프트사에서 사용자들에게 제 하는 방법으로서, TCP/IP와 같은 프로토콜 드라이버와 NIC 드라이버 사이에 끼워 어 방화벽, NAT(Network Address Translation) 등을 개발하는 방법이다.

(4) NDIS 후킹 필터 드라이버 : NDIS 라이브러리의 함수들을 후킹하는 방법으로 NdisRegisterProtocol, NdisDeregisterProtocol, NdisOpenAdapter, isCloseAdapter 및 NdisSend와 같은 함수들을 후킹하거나, 자신의 프로토콜 드라이 를 등록하는 NdisRegisterProtocol 함수를 사용하여 리턴된 NdisProtocolHandle을 준으로 TCP/IP와 같은 기존의 등록된 프로토콜 드라이버 링크를 찾아 NDIS와 통신 는 프로토콜 드라이버 및 NIC 드라이버의 I/O를 후킹하는 방법을 기반으로 한다.

본 발명에서 제시하는 인터넷 연결 방화벽은 상술한 커널 모드 소켓 필터, TDI 터 드라이버, NDIS IM 드라이버, NDIS 후킹 필터 드라이버 등에서 구현될 수 있으 . 일반적으로는 NDIS IM 드라이버 또는 NDIS 후킹 필터 드라이버에서 구현한다.

인터넷 연결 방화벽은 인터넷 연결 방화벽 컴퓨터에서 시작된 트래픽을 추적하 아이피와 포트의 모든 통신 테이블을 보관한다. 그리고, 인터넷의 모든 인바운드 트래픽은 이 통신 테이블에 존재하는 항목과 비교된다. 인바운드 인터넷 트래픽은 이블에 일치하는 항목이 있어서 통신 교환이 사용자의 컴퓨터에서 시작되었음을 입 하는 경우에만 인바운드 트래픽을 허용하고, 그러하지 아니한 경우에는 차단한다.

이와 같은 인바운드 트래픽의 허용은 후킹한 함수의 원본 주소를 그대로 호출함 로써 수행되고, 인바운드 트래픽의 차단은 원본 함수를 호출하지 않고, 원본 함수 호출이 성공 또는 실패하였다는 가짜 리턴을 함으로써, 또는, 원본 함수를 호출하 만 함수의 수행이 정상적으로 수행되지 않도록 잘못된 정보를 제공함으로써, 인바 드 트래픽을 차단한다.

상술한 방화벽과 관련된 기본적인 내용을 토대로 본 발명에서 제시하는 신뢰할 있는 프로세스를 허용하는 유연화된 네트워크 보안 시스템 및 그 방법에 대하여 명하도록 한다.

도 4는 본 발명에 따른 인터넷 연결 방화벽의 동작을 간략화한 흐름도로서, 포 감시부와 인터넷 연결 방화벽 설치 및 허용 프로그램 목록을 내부 허용 프로그램 장소에 저장하는 과정을 나타낸 흐름도이다.

먼저, 스텝 S410에서, 포트 감시부 및 인터넷 연결 방화벽을 설치한다.

이때, 포트 감시부는 TCP의 경우 소켓이 서버로 동작하기 위하여 리슨(Listen) 수행할 때, Winsock 후킹을 통하여 리슨 포트를 추출한다. 또는 msafd.dll에서 에 상응하는 연산이 발생하면, 또는, 이어서 커널의 소켓 부분인 AFD에서 이에 상 하는 연산이 발생하면, 또는, 이어서 TDI에 전달되고 TDI에서는 이에 상응하는 iSetEvent()를 통하여 TDI_EVENT_CONNECT가 호출될 때, 리슨하려는 포트를 추출한

그리고, 사용자 데이터그램 프로토콜(UDP : User Datagram Protocol)의 경우에 , 소켓에서 패킷을 받기 위하여 recvfrom을 호출하면, 유저 모드에서 Winsock 후킹 통하여 패킷을 받기 위한 서버 포트를 추출한다. 또는, 커널 모드에서 이어서 발 하는 AFD에서의 연산이 있을 때, 또는, TDI에서 이에 상응하는 TdiSetEvent()를 통 여 TDI_EVENT_RECEIVE_DATAGRAM이 발생할 때, 패킷을 받기 위한 서버 포트를 추출 다.

이와 같은 포트 감시부는 유저 모드에서 Winsock 후킹을 통하여, 또는, 커널 모 에서 커널 모드 소켓 필터, TDI 필터 드라이버를 통해서 설치하고, 서버 포트 보, 프로토콜 정보(TCP, UDP 등) 및 OPEN/CLOSE 정보를 추출하는 역할을 수행한다.

그리고, 인터넷 연결 방화벽을 설치한다. 이러한 인터넷 연결 방화벽은 상술한 와 마찬가지로, 커널 모드 소켓 필터, TDI 필터 드라이버, NDIS IM 드라이버, 윈도 즈 2000 필터 후크 드라이버, NDIS 후킹 필터 드라이버에서 구현될 수 잇고, 일반 으로는 NDIS IM 드라이버 또는 NDIS 후킹 필터 드라이버를 통하여 설치한다.

이어서, 스텝 S420에서, 허용 프로그램 목록을 내부 허용 프로그램 저장소에 저장한다. 도 5는 본 발명의 일 실시예에 따른 유연한 인터넷 연결 방화벽에서 통신용 프로그램 목록을 내부 허용 프로그램 저장소에 저장하기 위하여 디스플레이되는 인터페이스 화면을 보여주는 도면이다.

도 5에 도시된 바와 같이, 인터넷 연결 방화벽에서 허용할 프로그램을 선택하면 프로그램 이름, 프로그램 전체 경로 및 프로그램의 무결성 확인을 위한 해당 프로그램 파일의 MD5(Message Digest algorithm 5, 메시지 다이제스트 알고리즘 5) 해쉬값을 구한다. 이렇게 하여 얻어진 프로그램 이름, 프로그램 전체 경로 및 프로그램 MD5 해쉬값을 내부 허용 프로그램 저장소에 저장한다.

내부 허용 프로그램 저장소는 아래의 [표 1]과 같은 형태로 저장되며, 프로그램 이름, 프로그램 전체 경로 및 프로그램 MD5 해쉬값 정보를 포함하는 파일 또는 데이터베이스의 형태로 저장한다.

[표 1]

	프로그램 전체 경로	프로그램 MD5 해쉬값
	D:₩Program Files₩MSN Messenger₩msnmsgr.exe	0x83276482764827368682376482637872
	D:₩Program Files₩PcAnywhere₩PcAnywhere.exe	0x939472938742983794279739284793374

도 6은 본 발명에서 제시하는 인터넷 연결 방화벽 유연화 장치를 사용하는 전체 방화벽의 동작을 보여주는 블록도로서, 이를 상세히 설명하면, 다음과 같다.

인터넷 사용 프로그램(610)이 서버로 동작하기 위해서 서버 포트를 오픈하면, 터넷 연결 방화벽 기능 유연화 장치(620)는 해당 서버 포트를 오픈한 프로그램이 부 허용 프로그램 저장소(650)에 등록되어 있는 프로그램인지 여부를 판단한다.

해당 프로그램이 등록되어 있으면, 상기 인터넷 연결 방화벽 기능 유연화 장치 20)는 오픈한 서버 포트를 내부 허용 포트 저장소(660)에 등록한다.

한편, 외부로부터 인바운드된 트래픽이 전송되면, 상기 네트워크 카드(640)를 나서 상기 인터넷 연결 방화벽(630)으로 오게 된다. 상기 인터넷 연결 방화벽 기 유연화 장치(620)는 인바운드된 트래픽의 패킷을 조사하여 목적지 포트가 상기 내 허용 포트 저장소(660)에 등록되어 있는지 여부를 판단한다.

판단 결과, 해당 포트가 등록되어 있지 아니하면, 상기 인터넷 연결 방화벽 30)으로 패킷을 전송하며, 이 패킷은 차단될 것이다. 그러나, 해당 포트가 등록되 있으면, 상기 인터넷 연결 방화벽(630)을 통과시키지 아니하고, 상기 인터넷 연결 방화벽 기능 유연화 장치(620)로 우회시키기 위하여 후킹한 원본 함수를 호출한다.

아래의 [표 2]는 내부 허용 포트 저장소에 등록된 포트들을 보여주는 예이다.

표 2]

	프로그램 전체 경로	프로토콜	포트
	D:₩Program Files₩MSN Messenger₩msnmsgr.exe	TCP	1863
	D:₩Program Files₩MSN Messenger₩msnmsgr.exe	TCP	6891
	D:₩Program Files₩PcAnywhere₩PcAnywhere.exe	TCP	5631
	D:₩Program Files₩PcAnywhere₩PcAnywhere.exe	UDP	5632

상기 [표 2]에 도시되어 있듯이, 내부 허용 포트 저장소는 프로그램 전체 경로, 로토콜 및 포트 정보를 포함하며, 메모리 상에 배열 또는 연결 리스트로 존재하거나, 파일 또는 데이터베이스의 형태로 존재한다.

도 7은 본 발명의 일 실시예에 따른 유연한 인터넷 연결 방화벽의 내부 허용 포트 저장소에 서버 포트를 저장하고 삭제하는 과정을 나타낸 흐름도로서, 이를 상세히 설명하면, 다음과 같다.

먼저, 스텝 S701에서, 포트 감시부로부터 서버 포트, OPEN/CLOSE 정보 및 프로콜(TCP, UDP 등) 정보를 추출한 후, 스텝 S703에서, 포트 감시부에서 서버 포트를 요한 현재의 프로그램이 내부 허용 프로그램 저장소에 등록되어 있는 프로그램인지 부를 판단한다.

한편, 상기 스텝 S703에서 이와 같이 네트워크를 사용하는 현재 프로세스의 프로세스 정보를 얻어오는 방법은 포트 감시부에서 PsGetCurrentProcessId() 함수를 사용하여 현재의 프로세스 ID 정보를 추출한 후, 이 프로세스 ID를 통하여 현재 프로그램의 전체 경로를 얻어온다. 이렇게 얻어온 프로그램 전체 경로를 통하여 해당 프로그램의 MD5 해쉬값을 추출하며, 이 MD5 해쉬값과 프로그램 전체 경로로 현재의 프로그램이 내부 허용 프로그램 저장소에 있는지 여부를 판단하는 것이다.

상기 스텝 S703에서의 판단 결과, 등록되어 있지 아니하면 종료하고, 등록되어 있으면, 스텝 S705에서, 상기 추출한 OPEN/CLOSE 정보로 서버 포트의 OPEN/CLOSE 여부를 판단한다.

상기 스텝 S705에서의 판단 결과, 오픈된 포트이면, 스텝 S709에서, 프로그램 체 경로, 프로토콜 정보 및 서버 포트를 내부 허용 포트 저장소에 등록한 후, 종료다.

또한, 상기 스텝 S705에서의 판단 결과, 오픈된 포트가 아니면, 스텝 S706 및 텝 S707에서, 프로그램 전체 경로, 프로토콜 정보 및 서버 포트로 내부 허용 포트 장소에서 일치하는 항목을 찾아내어 삭제한 후, 종료한다.

도 8은 본 발명의 일 실시예에 따른 인터넷 연결 방화벽 이전에서의 패킷 처리 정을 나타낸 흐름도로서, 이를 상세히 설명하면, 다음과 같다.

먼저, 스텝 S801에서, 인터넷 연결 방화벽 이전에 인바운드 트래픽에서 패킷을 출한 후, 스텝 S803에서, 상기 추출된 패킷으로부터 인터넷 연결 방화벽 컴퓨터의 장에서 서버 포트에 해당 목적지(로컬) 포트와 프로토콜 정보를 추출한다.

그리고, 스텝 S805에서, 상기 추출한 목적지 포트와 프로토콜 정보가 내부 허용 트 저장소에 등록되어 있는지 여부를 판단한다.

상기 스텝 S805에서의 판단 결과, 등록되어 있지 아니하면, 스텝 S807에서, 해 패킷을 인터넷 연결 방화벽으로 전달하고, 등록되어 있으면, 허용해야 할 포트이로, 스텝 S809에서, 후킹한 원본 함수를 호출함으로써, 인터넷 연결 방화벽을 우회킨다.

위에서 양호한 실시예에 근거하여 이 발명을 설명하였지만, 이러한 실시예는 이 발명을 제한하려는 것이 아니라 예시하려는 것이다. 이 발명이 속하는 분야의 숙련에게는 이 발명의 기술사상을 벗어남이 없이 위 실시예에 대한 다양한 변화나 변경 E는 조절이 가능함이 자명할 것이다. 그러므로, 이 발명의 보호범위는 첨부된 청 범위에 의해서만 한정될 것이며, 위와 같은 변화에나 변경예 또는 조절예를 모두 함하는 것으로 해석되어야 할 것이다.

발명의 효과]

이상과 같이 본 발명에 의하면, 인터넷 연결 방화벽에 통신이 허용된 프로그램 사용하는 포트를 자동으로 추가 및 제거를 하게 함으로써, 전문 사용자가 아닌 일 사용자들도 쉽게 우수한 기능의 인터넷 연결 방화벽을 사용할 수 있게끔 하는 효 가 있다.

【특허청구범위】

【청구항 1】

네트워크 상에서 통신하기 위한 프로그램이 사용하는 서버 포트 정보를 추출하는 포트 감시 수단;

네트워크 사이에서 통신되는 정보의 제한 조건을 설정함으로써, 네트워크에 연결된 컴퓨터의 해당 네크워크 연결을 보호하는 방화벽(Firewall) 수단;

상기 방화벽 수단에서 통신을 허용하는 프로그램에 대한 정보를 추출하여 이를 등록하는 내부 허용 프로그램 저장 수단;

상기 내부 허용 프로그램 저장 수단에 등록되어 있는 프로그램이 사용하는 오픈된 서버 포트에 대한 정보를 상기 포트 감시 수단이 추출하면, 상기 추출된 서버 포트 정보를 등록하는 내부 허용 포트 저장 수단; 및

인바운드(Inbound)된 트래픽 패킷의 목적지 포트가 상기 내부 허용 포트 저장 수단에 등록되어 있는지 여부를 판단하여, 등록되지 아니한 포트이면 상기 방화벽 수단으로 전송하고, 등록되어 있는 포트이면 해당 패킷을 직접 해당 프로그램에 전송하는 방화벽 유연화 수단;

을 포함하여 이루어진 것을 특징으로 하는 신뢰할 수 있는 프로세스를 허용하는 네트워크 보안 시스템.

【청구항 2】

제 1 항에 있어서,

상기 내부 허용 프로그램 저장 수단이 추출하여 등록하는 프로그램 정보는 프로그램 이름, 프로그램 전체 경로 및 프로그램 MD5(Message Digest algorithm 5, 메시지 다이제스트 알고리즘 5) 해쉬값을 포함하는 것을 특징으로 하는 신뢰할 수 있는 프로세스를 허용하는 네트워크 보안 시스템.

【청구항 3】

제 1 항에 있어서,

상기 내부 허용 포트 저장 수단이 추출하여 등록하는 서버 포트 정보는 프로그램 전체 경로, 프로토콜 및 포트 정보를 포함하는 것을 특징으로 하는 신뢰할 수 있는 프로세스를 허용하는 네트워크 보안 시스템.

【청구항 4】

네트워크 사이에서 통신되는 정보의 제한 조건을 설정함으로써, 네트워크에 연결된 컴퓨터의 해당 네크워크 연결을 보호하는 방화벽(Firewall)을 이용하는 네트워크 보안 방법에 있어서,

네트워크 상에서 통신하기 위한 프로그램이 사용하는 서버 포트 정보를 추출하는 제 1 단계;

통신을 허용하는 프로그램에 대한 정보를 추출하여 등록하는 제 2 단계;

상기 제 2 단계에서 등록되어 있는 프로그램이 사용하는 오픈된 서버 포트에 한 정보를 상기 제 1 단계에서 추출하면, 상기 추출된 오픈 서버 포트 정보를 등록는 제 3 단계:

인바운드(Inbound)된 트래픽 패킷의 목적지 포트가 상기 제 3 단계에서 등록되 있는지 여부를 판단하는 제 4 단계:

상기 제 4 단계에서의 판단 결과, 등록되지 아니한 포트이면, 상기 방화벽으로 전송하는 제 5 단계: 및

상기 제 4 단계에서의 판단 결과, 등록되어 있는 포트이면, 해당 패킷을 직접 당 프로그램에 전송하는 제 6 단계:

를 포함하는 것을 특징으로 하는 방화벽을 이용하는 네트워크 보안 방법.

청구항 5】

제 4 항에 있어서,

상기 제 1 단계는,

TCP(Transmission Control Protocol)를 이용하는 통신인 경우, 소켓이 서버로 작하기 위하여 리슨(Listen)을 수행할 때, 후킹(Hooking)을 함으로써 리슨 포트를 출하는 것을 특징으로 하는 방화벽을 이용하는 네트워크 보안 방법.

청구항 6】

제 4 항에 있어서,

상기 제 1 단계는,

UDP(User Datagram Protocol)를 이용하는 통신인 경우, 소켓에서 패킷을 받기 하여 관련 함수를 호출하면, 유저 모드(User Mode)에서 후킹을 함으로써, 서버 포를 추출하는 것을 특징으로 하는 방화벽을 이용하는 네트워크 보안 방법.

청구항 7】

제 5 항 또는 제 6 항에 있어서,

상기 제 6 단계는,

후킹한 원본 함수를 호출함으로써, 해당 패킷을 직접 해당 프로그램에 전송하는 을 특징으로 하는 방화벽을 이용하는 네트워크 보안 방법.

청구항 8】

제 4 항에 있어서,

상기 제 2 단계에서 추출하여 등록하는 프로그램 정보는 프로그램 이름, 프로그 전체 경로 및 프로그램 MD5 해쉬값을 포함하는 것을 특징으로 하는 방화벽을 이용 는 네트워크 보안 방법.

청구항 9】

제 4 항에 있어서,

상기 제 3 단계에서 추출하여 등록하는 서버 포트 정보는 프로그램 전체 경로, 로토콜 및 포트 정보를 포함하는 것을 특징으로 하는 방화벽을 이용하는 네트워크 안 방법.

【구항 10】

네트워크 보안 방법을 실행할수 있는 컴퓨터로 읽을 수 있는 기록 매체에 있어

네트워크 상에서 통신하기 위한 프로그램이 사용하는 서버 포트 정보를 추출하 제 1 단계:

통신을 허용하는 프로그램에 대한 정보를 추출하여 등록하는 제 2 단계:

상기 제 2 단계에서 등록되어 있는 프로그램이 사용하는 오픈된 서버 포트에 한 정보를 상기 제 1 단계에서 추출하면, 상기 추출된 서버 포트 정보를 등록하는 3 단계:

인바운드(Inbound)된 트래픽 패킷의 목적지 포트가 상기 제 3 단계에서 등록되 있는지 여부를 판단하는 제 4 단계:

상기 제 4 단계에서의 판단 결과, 등록되지 아니한 포트이면, 방화벽으로 전송 는 제 5 단계: 및

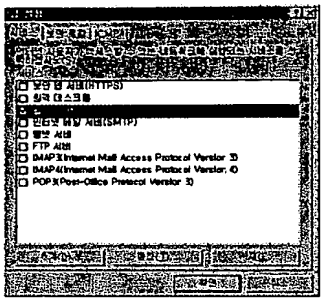
상기 제 4 단계에서의 판단 결과, 등록되어 있는 포트이면, 해당 패킷을 직접 당 프로그램에 전송하는 제 6 단계:

를 포함하는 것을 특징으로 하는 방화벽을 이용하는 네트워크 보안 방법을 실행
킬 수 있는 컴퓨터로 읽을 수 있는 기록 매체.

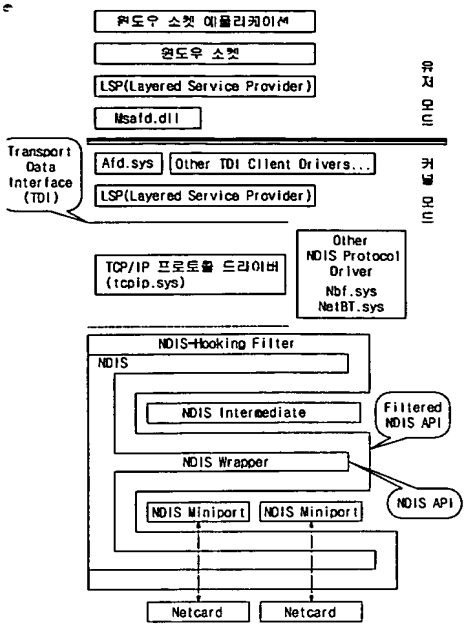
【도면】

【도 1】

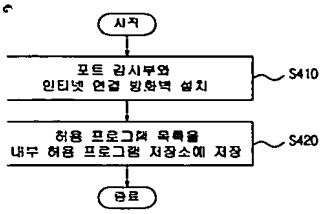
【도 2】


IMAP3(Internet Mail Access Protocol Version 3)
IMAP4(Internet Mail Access Protocol Version 4)
POP3(Post-Office Protocol Version 3)

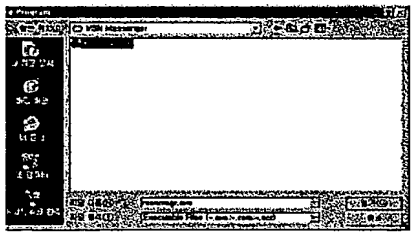
[도 3]


윈도우 소켓 애플리케이션
윈도우 소켓
LSP(Layered Service Provider)
Msafd.dll
유저 모드
Transport Data Interface (TDI)
Afd.sys
Other TDI Client Drivers...
LSP(Layered Service Provider)
커널 모드
TCP/IP 프로토콜 드라이버 (tcpip.sys)
Other NDIS Protocol Driver
Nbf.sys
NetBT.sys
NDIS-Hooking Filter
NDIS
NDIS Intermediate
Filtered NDIS API
NDIS Wrapper
NDIS API
NDIS Miniport
NDIS Miniport
Netcard
Netcard

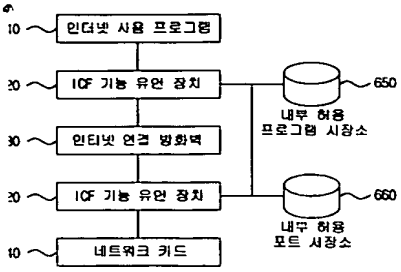
[도 4]


시작
포트 감시부와
인터넷 연결 방화벽 설치
S410
허용 프로그램 목록을
내부 허용 프로그램 저장소에 저장
S420
종료

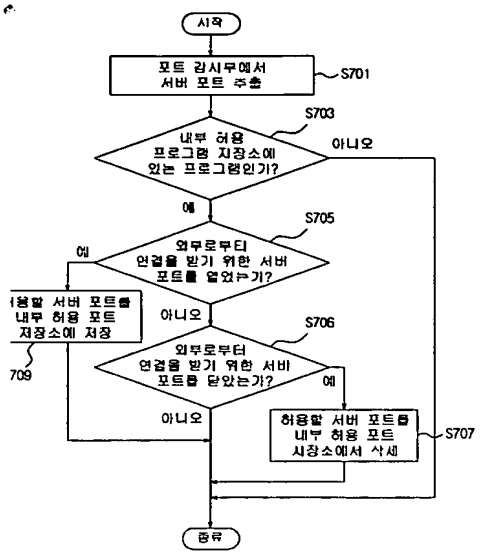
[도 5]



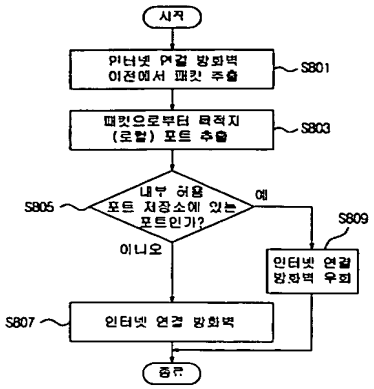
도 6)


610
인터넷 사용 프로그램
620
IOF 기능 유연 장치
650
내부 허용
프로그램 시장소
630
인터넷 연결 방화벽
620
IOF 기능 유연 장치
660
내부 허용
포트 시장소
610
네트워크 카드

도 7]


시작
포트 감시부에서 서버 포트 추출
S701
내부 허용 프로그램 저장소에 있는 프로그램인가?
S703
아니오
예
외부로부터 연결을 받기 위한 서버 포트를 열었는가?
S705
예
아니오
용할 서버 포트를 내부 허용 포트 저장소에 저장
709
외부로부터 연결을 받기 위한 서버 포트를 닫았는가?
S706
예
아니오
허용할 서버 포트를 내부 허용 포트 저장소에서 삭제
S707
종료

[도 8]


시작
인터넷 연결 방화벽 이전에서 패킷 추출
S801
패킷으로부터 목적지 (로컬) 포트 추출
S803
내부 허용 포트 저장소에 있는 포트인가?
S805
예
아니오
S809
인터넷 연결 방화벽 우회
S807
인터넷 연결 방화벽
종료